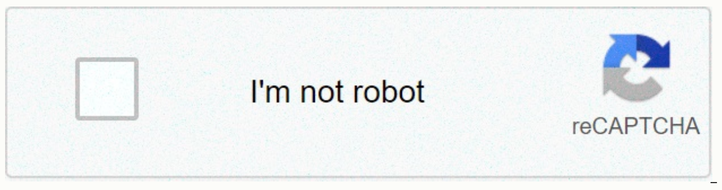

Continue

Check point 5100 datasheet

Skip to the Go to Security Gateway content of the top 1 checkpoints 5200 CHECK POINT Datasheet. 5200 Next Generation Security Gateway . FOR SMALL BUSINESS AND BRANCH. CHECK POINT 5200 FOLLOWING SUMMARY. Generation security Check Point 5200's next-generation security gateway combines Gateway's most comprehensive security protections to protect your small business and branch office deployments. The 5200 is a next-generation 1UU security gateway with an I/O expansion slot for increased port capacity, An optional 500GB (HDD) or 240GB (SSD) disk and optional small business and branch office light management (LOM) for remote management.2 This powerful next-generation office security security gateway is optimized to deliver real-world threat prevention to protect your critical assets and environments. Product benefits High-performance protection against comprehensive threat prevention. The most advanced cyberattacks The rapid growth of malware, the increasing sophistication of attackers and the rise of the new single prevention for the first time for unknown zero-day threats require a different approach to keep the most sophisticated enterprise networks zero-day attacks and data secure. Check Point offers full integration, Comprehensive Threat Optimized to inspect SSL Prevention with award-winning SandBlast Threat Emulation and Threat Extraction encrypted traffic for complete protection against the most sophisticated threats and technology vulnerabilities prepared for the future of zero day.3 Protects against the risks of future Centralized Control and LOM Unlike traditional solutions that are subject to evasion techniques, introduce unacceptable delays in serviceability, or allow potential threats when evaluating files, Check Modular, the expandable chassis point with Sand Sand. With our solution, flexible I/O options, your employees can work safely no matter where they are and don't compromise their productivity. Product Features Simple deployment and management Secure remote access to HIGHLIGHTS corporate PERFORMANCE.4 Resources from a wide variety of IPS Firewall NGFW 1 Threat Prevention 2. 16 Gbps 3 Gbps Gbps devices A network expansion slot to add measured performance under ideal test conditions. Additional performance details on page 4. 1. Includes Firewall, Application Control and IPS Software Blades. port density, fiber, and open-failure I/O. 2. Includes firewall card options, Application Control, URL Filtering, IPS, Antivirus, Anti-Bot and SandBlast Zero-Day Protection Software Sheets using redundant device clustering technologies a single point of failure 2018 Check Point Software Technologies Ltd.5 All rights reserved. [Protected] Non-confidential content ? May 15, 2018 Page 1. Check Point 5200 Security Gateway (Check Point 5200 Security Gateway) Datasheet ALL SECURITY SOLUTIONS INCLUDED INSPECT ENCRYPTED CONNECTIONS. Check Point 5200 next-generation security gateways offer a shift towards increased use of HTTPS, SSL, and complete and consolidated security solution available in two ciphers to increase Internet Security. At the same time full packages: files delivered to your organization via SSL and TLS. NGTP: Avoid sophisticated cyber threats with represent a stealth attack vector that bypasses traditional application control, URL filtering, IPS, antivirus, security deployments.6 Check Point Threat Prevention Anti-Bot and Email Security . Search within encrypted SSL and TLS tunnels to detect NGTX: NGTP with SandBlast Zero-Day Protection, threats, ensuring that users remain in compliance with the enterprise, including threat and threat emulation policies while browsing the Internet and using corporate data. Extraction. HIGH PERFORMANCE PACKAGE INCLUDED. PREVENT KNOWN THREATS AND ZERO-DIA Customers with high connection capacity requirements can The 5200 Next Generation Security Gateway protects the purchase of the affordable High Performance Package (HPP).7 Organizations of known and unknown threats with This includes the base system plus a 4x 1Gb SFP. Antivirus, Anti-Bot, SandBlast Threat Emulation interface card, transceivers, Lights-Out-Management and 16. (sandboxing) and SandBlast threat extraction technologies. GB of memory for high connection capacity. As part of Check Point's SandBlast zero-day protection base HPP Max solution, the cloud-based threat emulation engine detects 1 GbE (copper) 6 6 14 ports. malware in the exploit phase, even before hackers can apply 1 GbE (fiber) ports 0 4 4. evasion techniques that attempt to bypass sandbox.8 File Transceivers (SR) 0 4 4. they are quickly quarantined and inspected, running in a virtual sandbox to uncover malicious behavior before it enters its 8GB 16GB 16GB RAM. Network. This innovative solution combines cloud-based AC or DC power units 1 1 1. CPU-level inspection and operating system-level sandboxing to prevent optional output light management including infection including the most dangerous vulnerabilities, and zero-day and targeted attacks. REMOTE MANAGEMENT AND SUPERVISION. In addition, an optional Lights-Out-Management (LOM) card also provides SandBlast Threat Extraction eliminates out-of-band remote management to remotely diagnose, start, exploitable content, including active content, and restart and manage next-generation security gateway objects, rebuild files to eliminate potential threats, and from a remote location.9 Administrators can also use the LOM. quickly delivers disinfected content to users to maintain the web interface to remotely install an operating system

image from an ISO. business flow. NGTX. NGTP. (SandBlast) SECURE REMOTE ACCESS. Avoid Known Prevent Known Each next-generation Check Point security gateway is a zero-day threat configured with mobile access connectivity for up to 5 users, attacks using the mobile access sheet. This license provides secure remote firewall access to corporate resources from a wide variety of VPN (IPsec) devices, including smartphones, tablets, PCs, Macs, and Ips. Integrated application control security management. URL filtering Each Check Point device can be managed locally by Anti-Bot with the built-in security management available 1 or through central unified management. Using local management, Antivirus . the device can manage itself and an adjacent anti-spam device. highly available deployments. SandBlast Emulation Threat . Removing SandBlast 1 threats. not available when purchased with SSD 2018 Check Point Software Technologies Ltd. All rights reserved. [Protected] Non-confidential content ? May 15, 2018 Page 2. The Check Point 5100 appliance combines the most comprehensive security protections to protect your deployment from small and branch offices. The 5100 is a 1 U device with an I/O expansion slot for high port capacity, a 500 GB h ard disk, and optional lights - Out Management (LOM) for remote management. This powerful security appliance is optimized to deliver real-world threat prevention to protect your critical assets and environments. Comprehensive threat prevention Rapid malware growth, increasing attacker sophistication, and the rise of new unknown zero-day threats require a different approach to maintaining business networks and data healing. Check Point offers comprehensive and comprehensive threat prevention with award-winning SandBlast™ threat emulation, and threat extraction for complete protection against the most sophisticated threats and zero-day vulnerabilities. 1U rack mount. Up to 14x1GbE ports. Up to 16 GB of memory. 425 SecurityPower* 5.3 Gbps Firewall Performance 250 Mbps NGTP Performance 16 Gbps Firewall Performance (1518 bytes UDP) 1.88 Gbps VPN Performance (AES-128) 3.2 Million / 6.4 Million with Simultaneous RAM Connections (HPP) Product Benefits Allow Product Benefits Allow Security More advanced for threat prevention Optimal performance even when inspecting SSL encrypted traffic Future-proof technology protects against the risks of future Centralized Control and LOM improves serviceability High Performance Package optimizes platform performance Modular and scalable chassis with flexible I/O options Product features Simple deployment and management Secure remote access to corporate resources from a wide variety of devices A network expansion slot to add port density , fiber and open failure I/O card options Redundant device clustering technologies eliminate a single point of failure The most advanced threat prevention security Comprehensive protections include firewall, IPS, application control, antibot, URL filtering and award-winning sandboxed technology in Check Point SandBlast Zero-Day Protection Next Generation Threat Prevention package provides uncompromising protection against known threats SandBlast threat prevention provides the most advanced protections against unknown threats, vulnerabilities and zero-day attacks Full protection without compromise Hardware and software optimized for Complete advanced threat prevention security, including SSL encrypted traffic inspection Up to 1,000 Mbps of real-world threat prevention performance Up to 22 Gbps of Modular real-world firewall performance, Expandable Chassis Design Optional Chassis Design Optional redundant power supplies reduce single points of failure Centralized control with Lights-Out-Management (LOM) for greater flexible I/O service capacity with a choice of 40 Gigabit Ethernet (GbE) Check Point 5000 devices offer complete and consolidated security available in two packages: Next Generation Threat Prevention (NGTP): Prevention of sophisticated cyber threats with IPS, application control, antivirus, anti-bot, URL filtering and SandBlast Threat Prevention email security (NGTX) : Next Generation Advanced Zero-Day Threat Prevention: NGTP with Threat Emulation and Threat Extraction Prevents Unknown Threats 5000 devices are designed to protect branch offices from known and unknown threats with antivirus with antivirus, anti-bot, SandBlast Threat Emulation (Sandboxing) and Sand ThreatBlast Extraction technologies. As part of Check Point's SandBlast zero-day protection solution, the cloud-based threat emulation engine detects malware in the exploit phase, even before hackers can apply evasion techniques that attempt to bypass the sandbox. Files are quickly quarantined and inspected, running in a virtual sandbox to detect malicious behavior before it enters the network. This innovative solution combines CPU-level cloud-based inspection and operating system-level sandboxing to prevent infection from the most dangerous vulnerabilities and targeted, zero-day attacks. In addition, SandBlast Threat Extraction removes exploitable content, including active content and embedded objects, rebuilds files to eliminate potential threats, and quickly delivers disinfected content to users to maintain business flow. Optional high-performance package Customers with high connection capacity requirements can purchase the affordable high-performance package. This includes the device plus an interface card with transceivers and Lights-Out-Management. Flexible connectivity options High-speed connectivity is essential to meet the needs of today's business networks. That's why 5000 devices are built to provide maximum port density and flexible connectivity in a compact single rack unit format, including support for 4x1GbE, 4x10GbE (5600 and 5800), as well as 2x40GbE (5800). Remote management and monitoring One Optional LOM provides out-of-band remote management to diagnose, start, restart, and manage the device from a remote location. Administrators can also use the LOM web interface to remotely install an operating system image from an ISO file. A reliable and useful platform Check Point 5000 devices offer business continuity and ease of service through optional features such as hot-swappable redundant power supplies as well as advanced lights-Out (LOM) management for out-of-band management. En En these features ensure a greater degree of business continuity and ease of service for customer networks. Integrated security management Each Check Point device can be managed locally through its available integrated security management or centrally through unified management. An intuitive web-based management interface provides local management of up to two,5000 devices for highly available deployments. 5100 Security Appliance Management 10/100/1000Base-T RJ45 port RJ45/micro USB console port One network card expansion slot 5x 10/100/1000Base-T RJ45 ports 2x USB ports for ISO installation Lights-Out Management port Appliance 5200 5400 5600 5800 Security Power 425 600 950 1750 Firewall Throughput (Gbps) 5.3 10 17.5 22 IPS throughput (Gbps) 810 Mbps 1.08 1.9 3.05 NGFW throughput (Gbps) 520 Mbps 690 Mbps 1.18 2 Threat prevention (Gbps) 250 Mbps 330 Mbps 540 Mbps 1 Firewall, 1518 byte UDP (Gbps) 16 22 25 35 Connections per Second (K) 125 150 185 185 Concurrent Connections (M)2 3.2/6.4 3.2/6.4 3.2/6.4 3.2/6.4 VPN AES-128 Throughput (Gbps) 1.88 2.16 6.5 10 IPS throughput (Gbps) 3 3.9 7.8 10 NGFW throughput (Gbps) 2.7 3.4 5.8 8.1 VS Supported (Default/Max)2 10/20 10/20 10/20 10/20 10/100/1000Base-T Ports 6/14 10/18 10/18 10/26 1000Base-F SFP Ports 0/4 0/4 0/4 0/8 10GBase-F-SFP+ Ports 0/0 0/0 0/4 0/8 40GBase-F SFP+ Ports 0/0 0/0 0/0 0/4 Memory 8 ,16 8, 16 8, 16 8, 16 Storage 1x 500 GB 1x 500 GB 1x 500 GB 1x 500 GB I/O expansion slots 1 1 1 2 Optional Optional Out-Management Lights Optional Optional Enclosure Included 1U 1U 1U Dimensions (wxdxh standard) 17.24 x 16.01 x 1.73 in. 17.24 x 16.01 x 1.73 in. 17.24 x 20 x 1.73 in. 17.24 x 20 x 1.73 in. Dimensions (metric wxdxh) 438 x 406.55 x 44 mm 438 x 406.5 x 44 mm 438 x 508 x 44 mm 438 x 508 x 44 mm Weight 6.22kg (13.7 lbs) 6.37kg (14 lbs) 7.95kg (17.53 lbs) 8.37kg (18.45 lbs) Operating Environment 0°C - 40°C at 5 - 95% relative humidity Non-Operating Environment (-20)°C - 70°C at 5 - 95% relative humidity Dual, Hot-Swap Power Supplies NA NA Optional Optional Power Input 90 - 264VAC (47-63HZ) Single Power Supply Rating 250W 250W 275W 275W Power Consumption (Max) 62.9W 76.5W 103W 110W Safety UL60950-1, CB IEC60950-1, CE LVD EN60950-1, TUV GS Emissions CE, FCC, VCCI, RCM/C-Tick Environmental RoHS II, *REACH, *ISO14001 1assumes maximum production throughput with real-world traffic blend, a typical rule-base size , NAT and LOGGING enabled and most secure threat prevention protection 2 performance measured with default memory /maximum Software Blade NGTP NGTX Firewall Identity Awareness IPSec VPN Advanced Networking & Clustering Mobile Access 1 IPS Application Control URL Filtering Antivirus Anti-Bot Anti-Spam & Email Removing security threats * Threat emulation * DLP * * SmartEvent status and network policy management log * * SmartWorkflow* * * * Management Portal * * User Directory * * SmartProvisioning * SmartReporter * * Endpoint Policy Management * * Compliance * * NGTP - Next Next Threat Prevention; NGTX - SandBlast Threat Prevention; - Included* - Optional 1 Five users are included in the default package